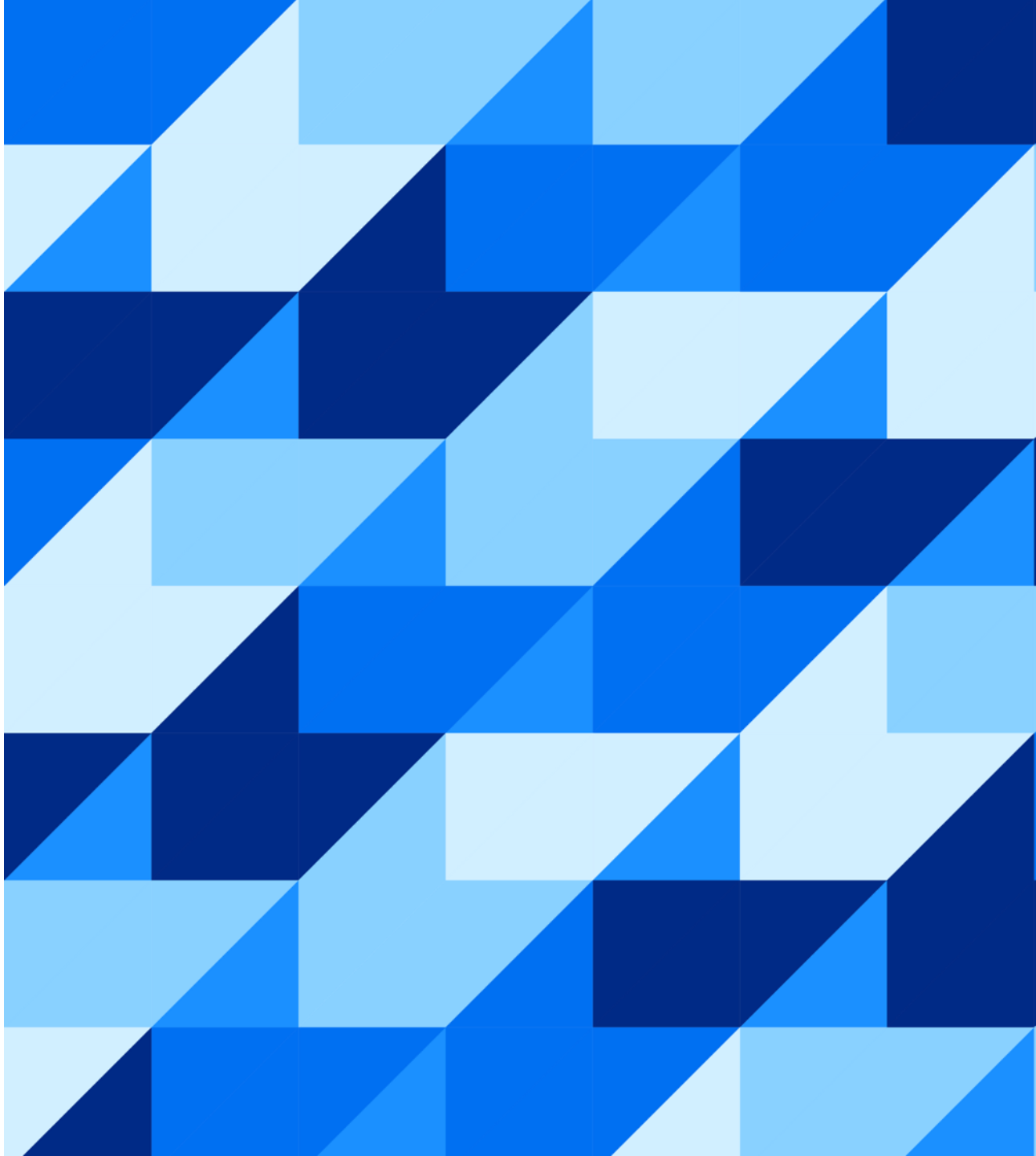
Der EU Cyber Resilience Act und Open Source: Wie SAP reagiert

Sebastian Wolf, SAP
12. September 2024

Public



Der Cyber Resilience Act – Was steckt drin?

- Von der EU-Kommission im Spätsommer 2022 ins Leben gerufen, aktuell im finalen Abstimmungsprozess vor der Verkündung Ende 2024
- Reguliert den EU-Marktzugriff:
  - Nur konforme Produkte dürfen verfügbar gemacht werden
  - Benötigt Konformitätszertifikat (CE-Zeichen)
- Alle Produkte mit digitalen Elementen (Hard- und Software) sind betroffen
  - Regelgerechtes Handling von Cybersicherheit und Schwachstellen über den gesamten Produktlebenszyklus
  - Weitergehende Transparenz bei der Software-Stückliste
- Risikobasierte Prüfung auf Konformität

Übergreifendes Ziel:
Unternehmen und Bürger vor Cyberattacken schützen!

Geltungsbereich

Produkte mit digitalen Elementen laut CRA

- **Hardware und Komponenten**, die eigenständig auf den Markt gebracht werden (Laptops, Smart-Devices, Telefone, Netzwerkausrüstung, CPUs etc.)
- **Software und Komponenten**, die eigenständig auf den Markt gebracht werden (Betriebssysteme, Office-Suites, Spiele, Apps etc.)
- Definition beinhaltet Lösungen mit **Remote-Datenverarbeitung!**

Nicht im Geltungsbereich

- Nicht-kommerzielle Produkte (z.B. **Open Source außerhalb von kommerziellen Aktivitäten**)
- Dienste, insbesondere Cloud/Software-as-a-Service (von NIS2 abgedeckt)
- Bestimmte Produkte, die bereits hinsichtlich Cybersecurity reguliert sind (z.B. Autos, medizinische Geräte, zertifizierte aeronautische Geräte)

Abgrenzung für einzelne Punkte aus unserer Sicht schwierig, zentrale offene Fragen:

- Was ist kommerzielle Aktivität bei Open Source-Software?
- Welche Akteure können als „Open Source-Stewards“ agieren, welche Aufgaben haben sie genau?
- Was ist Remote-Datenverarbeitung (relevant für CRA) und was ist SaaS/Cloud-only (nicht relevant)?

Mutmaßliche Auswirkungen auf SAP (und jeden anderen Marktteilnehmer)

Neue Verpflichtungen

- Reporting von Security-Incidents und aktiv ausgenutzten Schwachstellen
- Ausrichtung des Software-Entwicklungsprozesses auf neue Cybersecurity-Anforderungen
- Stringente technische Dokumentation für alle Produkte
- Überwachung durch nationale Marktüberwachungsbehörden
- Konformitätsprüfungen, müssen zudem bei wesentlichen Änderungen erneuert werden

Kosten für Compliance

- Produktentwicklung und Tests
- Dokumentation
- Konformitätsprüfung durch Drittanbieter
- Reporting
- Preiserhöhung/Lizenzänderungen bei verwendeten Komponenten

Folgen bei Non-Compliance

- Verbot oder Beschränkungen bei der Inverkehrbringung sowie Geldstrafen

Open Source-Software steckt in über 95% der Produkte, viele eigene OSS-Projekte

Korrektes Handling von Open Source elementar!

Wie begleitet SAP die Gesetzgebung?

Wir unterstützen die Ziele des Cyber Resilience Acts

- Erhöhte Widerstandsfähigkeit gegen Angriffe, schnellere Reaktionsfähigkeit etc.
- Sicherung der Software-Lieferketten

Wir sehen Unklarheiten und Risiken insbesondere bei Open Source

- Was macht kommerzielle Aktivität bei Open Source-Software aus?
- Verfügbarmachung auf dem Markt auch bei freien Lizenzen?
- Welche Organisationen können OSS-Stewards im Sinne des CRA sein?

Unsere Position im Zuge der Gesetzgebung und Richtlinienbestimmung

- Trennung Up-/Downstream Open-Source
- Upstream immer von CRA ausgenommen. Open Source-Anbieter sollen keine „Hersteller“ nach CRA sein
- Markteintritt formal erst mit Paketierung, nicht mit Veröffentlichung des Quellcodes
- Unternehmen sollen auch als Open Source-Stewards agieren können

Was erwartet uns in der Zukunft?

Die Softwareindustrie wird erstmals zu einem regulierten Markt

- Open Source-Software wird über Produkte ebenso der Regulierung unterworfen
- Bei Open Source stellen sich die Fragen:
  – Wer ist für die Konformitätserklärungen verantwortlich?
  – Wie bezahlen wir die Zertifizierung und alle zugehörigen Maßnahmen?

Höhere Kosten sicher, andere Auswirkungen unklar

- Wird jede Firma einzeln die verwendeten OSS-Komponenten zertifizieren?
  – Kurzfristig vielleicht ja, aber sehr ineffizient und insgesamt sehr teuer
- Mittel-/Langfristig werden sich auf dem Markt Synergien ergeben (müssen)
  – Verstärkte Rolle der Open Source-Foundations und Zusammenarbeit von Firmen
  – Kommerzielle Forks/Distributionen/Supportmodelle für OSS-Komponenten
- Open Source-Ökosystem und EU-Standort könnten nachhaltigen Schaden nehmen
  – Abhängig von Durchführungsbestimmungen
  – Besondere Gefahr für Distributionsplattformen und dadurch Rückzug vom EU-Markt (siehe KI-Regulierung)

Wie bereitet sich SAP vor, was können wir empfehlen?

Analyse bestehender Prozesse und deren Verbesserung

- SAP setzt bereits lange Zeit umfangreiche Entwicklungs- und Betriebsprozesse um:
  – Verbindliche Richtlinien zur Verwendung von OSS-Komponenten
  – Fokus auf kompatible Lizenzen, Sicherheit/Vermeidung von Schwachstellen
  – Verbesserungen bei anderen Risiken (z.B. Lieferkette) aktuell im Gange
- Ziele analog zum CRA, da im Interesse von SAP, Partnern und Kunden
- Maßnahmen jetzt schon notwendig (Lizenzmanagement, Exportkontrolle etc.)

Unsere Empfehlungen an Sie

- Systematisches Management aller Softwarekomponenten in Software-Stücklisten
- Open Source-Foundations stärken (Mitgliedschaft, eigene Contributions etc.)
- Produktentwicklungsrichtlinien auf eigene OSS-Projekte anwenden
- Zeitnah mit Analyse und Umsetzung beginnen
  – Erlaubt das Strecken von Investitionen auf mehrere Jahre
  – Wettbewerbsvorteil möglich (Know-How, positive Außenwirkung, ggf. neue Geschäftsmodelle)

Zusammenfassung und Schlussfolgerungen

Der CRA hat große Auswirkungen auf die Software-Industrie

- CE-Zeichen jetzt für alle Softwareprodukte, Konformitätserklärung notwendig
- Betrifft den kompletten Software-Lebenszyklus
- Open Source-Ökosystem mittelbar besonders betroffen:
  – Alle Komponenten müssen bei Einsatz in Produkten ebenfalls CRA-konform sein
  – Es gab bisher keine einheitlichen Qualitätskriterien für freie Projekte
  – Abgrenzung kommerzielle/nicht-kommerzielle Aktivität noch unklar
  – Abschreckung von OSS-Projekten möglich
- Auswirkungen ggf. sogar noch umfangreicher als die DSGVO

Umfangreiche Vorbereitungen trotz Unklarheiten rechtzeitig angehen

- Der CRA wird kommen und alle betreffen, die in der EU Software verkaufen wollen
- Regularien könnten noch entschärft werden (z.B. für Cloud, eigene OSS-Projekte)
- Aber: Ziele und Maßnahmen des CRA weitgehend sinnvoll und zielführend
- Deswegen: Bei offensichtlichen Lücken jetzt Maßnahmen vorbereiten/umsetzen!

Vielen Dank!

Kontakt-Information:

Sebastian Wolf
sebastian.wolf@sap.com

SAP Open Source Program Office
ospo@sap.com